BOC Cloud Services - Encryption

Table of contents

1 Acronyms

Acronym	Description
DEK	Database Encryption Key
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
IaaS	Infrastructure-as-a-Service
PII	Personally Identifiable Information
RSA	Rivest–Shamir–Adleman
SaaS	Software-as-a-Service
TLS	Transport Layer Security

2 Introduction

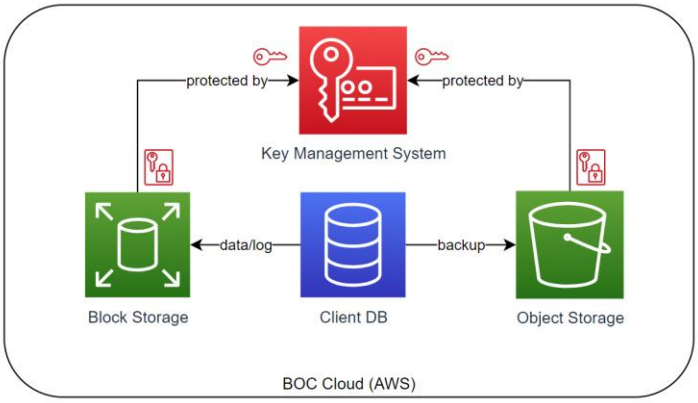
BOC is processing confidential data and, in some cases, Personally Identifiable Information (PII) in their cloud environments on behalf of Software-as-a-Service (SaaS) clients. To support the clients in fulfilling regulatory requirements with respect to protection of the data, BOC offers different options to encrypt Data at Rest.

Data in Transit is always protected by state-of-the-art technologies such as TLS, IPSec – it is never transmitted over public networks without applying encryption.

3 Default encryption on block devices and in object storage

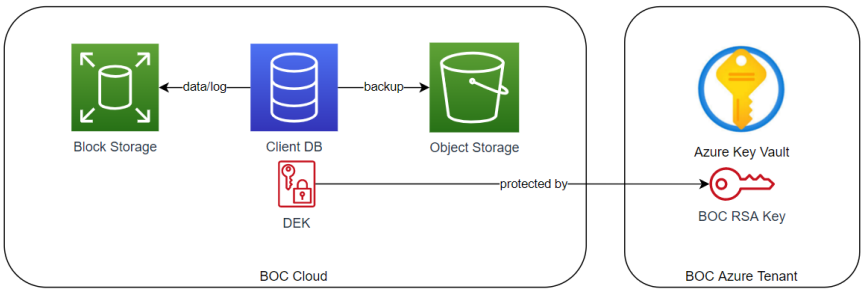
Whenever the Infrastructure-as-a-Service (IaaS) provider supports it, storage is encrypted by default using a key owned by BOC and managed in the IaaS provider's FIPS 140-2 Level 2 (or better) Key Management Service. The applied encryption method is AES-256. This is the case for the following BOC Cloud locations:

- Frankfurt, Germany (AWS)
- Paris, France (AWS)



4 Database encryption – Option 1 – BOC key managed in Azure Key Vault

Enterprise clients can request that BOC enables encryption of the database used by the clients' SaaS accounts at any time. In this scenario the Database Encryption Key (DEK) is protected by an RSA key managed within an HSM-backed Key Vault in BOC's Azure Tenant. This option provides the protection compliant with FIPS 140-2 Level 2. The actual data encryption is done using the AES-256 standard. This option is available in all BOC Cloud locations.

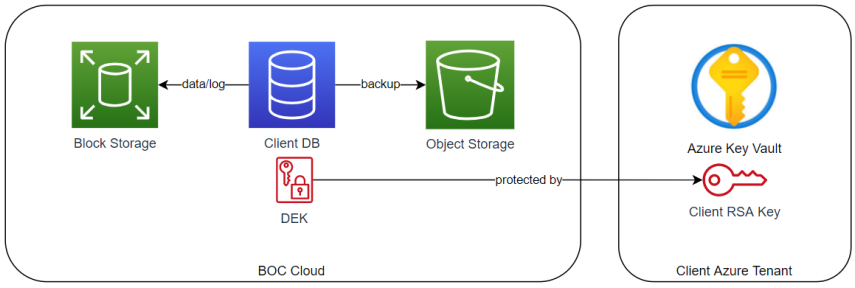


5 Database encryption – Option 2 – Hold Your Own Key (HYOK) in Azure Key Vault

In situations where the client prefers to have their own key material used to protect the DEK, the preferred option is to apply the Hold Your Own Key (HYOK) model. In such a scenario, the client manages a Key Vault in their Azure Tenant and dedicates a key to be used for the SaaS database.

To setup this model, an App Registration needs to be created in the tenant's Azure AD representing the SaaS account in BOC's cloud environment and a Secret (consisting of the Application ID without hyphens and the client secret for the application registration) needs to be created for this application. In the client's Key Vault, a key needs to be created and the registered Application needs to be granted with the *get*, *wrapKey,* and *unwrapKey* privileges for that key. The Key Vault name, the Key name, and the Secret need to be transmitted to BOC over a secure channel.

BOC then configures the database encryption to use the client's key for encrypting and decrypting the DEK whenever needed. The encryption standard applied to the actual data is AES-256. This option is available in all BOC Cloud locations.



6 Database encryption – Option 3 – Bring Your Own Key (BYOK)

As an alternative to HYOK, the Bring Your Own Key (BYOK) model can be applied, provided that the client can export a key from one of the supported HSM models, see https://docs.microsoft.com/azure/key-vault/keys/hsm-protected-keys for details.

Using such a key, BOC can protect the DEK with the client's key material managed in a FIPS 140-2 Level 2 compliant Key Vault in BOC's Azure tenant. For business continuity reasons, BOC may request two key exports from the client's HSM in order to import the key in two independent Key Vault instances.

Data encryption is done with AES-256 standard. This option is available in all BOC Cloud locations.